# Technology Drivers for Flight Telerobotic System Software



**Robert Labaugh**
**SET Group**
**Denver, Colorado**

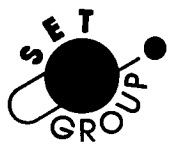
# Technology Drivers for Flight Telerobotic System Software

Robert J. LaBaugh
SET Group
Denver, Colorado



## Selected Topics In
## Robotics For Space Exploration

3/18/93 LaRC

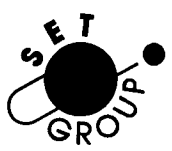


## Introduction

- Major Software Drivers in a Flight Manipulator System
  - Control Algorithms
  - Distributed Hardware Architecture
    - Bus Loading
    - Margin/Performance Requirements (10ms/20ms)
  - Data Management
    - Telemetry/Data Recording
    - Operator Interface
  - Safety
  - Fix It in Software







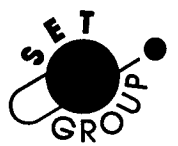
## Flight Software Lines of Code

- Estimated at 40K Ada Statements
- Approximately 22K in Development Library at Start of Technology Capture Effort

| Function | Lines of Code | Percentage |
|---|---|---|
| Control Algorithms | 5.5K | 13.8% |
| Operator Interface | 10.0K | 25.0% |
| Safety | 5K | 12.5% |
| Data Management | 7K | 17.5% |
| Misc. Hardware Control | 5.5K | 13.8% |
| Common Utilities | 5K | 12.5% |
| ROM | 2K | 5.0% |







# Flight Computer Architecture

- Distributed 80386-80387s
  - 8 Controllers
    - Custom Design
    - 512K Bytes RAM
    - Joint Controllers Embedded in Arm
    - 4x4 in. Surface Mount Boards
  - Space Station Standard Data Processor
    - 3 CPUs with 4M Bytes RAM each
- MIL-STD-1553B Busses Connecting CPUs
  - Workstation Bus
  - Telerobot Bus
- PGSC Used for Display and Initial Program Load





## System Safety

- Critical Items Required To Be Two Fault Tolerant
  - One Path Outside of Computer System
  - Other Two in Independent Systems
- FTS Safety Requirements
  - Safe Return Of Orbiter
    - Doors Must Be Able To Close
    - System Must Be Safe For Landing (Caged)
  - Inadvertent Release of Hardware
    - Manipulator Grasp of Object
    - Object Caging Mechanism
  - Correct Operation of Manipulator
    - No Unplanned Contact with Environment
    - Planned Contact at Safe Forces and Torques

# Safety Critical Parameters

| Parameter | Monitored By | Hazard Mitigated |
|---|---|---|
| Cartesian Position | TRCC/TRRC | Unplanned Contact |
| Cartesian Velocity | TRCC/TRRC | Unplanned Contact |
| Cartesian Force (6 DOF) | Joint Controllers (H/W) | Excessive Force |
| Joint Position | Joint Controllers (H/W)/TRRC | Unplanned Contact |
| Joint Velocity | Joint Controllers/TRRC | Unplanned Contact |
| Joint Torque | Joint Controllers (H/W) | Unplanned Contact, Excessive Force |
| Joint Motor Current | Joint Controllers (H/W) | Unplanned Contact, Excessive Force |
| End Effector Gripping Force | Joint Controllers (H/W) | Excessive Force |
| End Effector Grip Current | Joint Controllers (H/W) | Excessive Force |
| Joint Position Variance | Joint Controllers | Unplanned Contact |
| FTT-A versus FTT-B Variance | TRCC | Excessive Force |
| Actuator/EE Temperature | TRCC | Failure to Stow |
| Processor Temperature | TRCC | Failure to Stow, Unplanned Contact |
| Processor Health | TRCC/TRRC/PM | Unplanned Contact |





## System Safety – Software Functions

- Cartesian Safety
  - Position/Boundary Management
    - Check Arm Position versus Environment
  - Velocity Limits
  - Force Applied to Environment
- Manipulator Joint Safety
  - Position versus Joint Stops
  - Consistency of Three Position Sensors
- Communications
  - Heartbeat Between Critical Computers
  - Checksum of All Messages
- Temperatures

## System Safety – Software Functions (cont.)

- Operational Checks
  - Tighter Bounds than Safety Limits
  - Violation Results in Limited Value or Soft Stop
- Safety Checks
  - Violation Results in Emergency Shutdown
- Hardware Checks Can Also Produce Emergency Shutdown (ESD)
  - Need to Report Sensor Which Caused ESD
- Ada Run-time Checks Not Sufficient for Detection of Problems
  - Corruption of Code
  - Execution of Non-code
- DDC-I Use of 80386 Protected Mode
  - Code in Read Only Segment
  - Access Outside of Segment Trapped by Hardware





## Fix It in Software

- Coarse Encoder Calibration Curves
  - Position Dependent Error
  - Varied with Temperature
  - Varied with Time
- Augmented Damping
  - 1000Hz
  - Multiple Digital Filters
- FTT Decoupling
- Safety
  - Force Limiting
  - Third Instance of Collision Avoidance
- Power Switch Control
- Power/Thermal Problem